ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 28, Number 1, Spring 1998

SOME ALGEBRA OF NEWTON POLYNOMIALS

D.G. MEAD AND S.K. STEIN

0. Introduction. For the positive integer k, N_k denotes the Newton polynomial $x^k + y^k$. Let $Q(x, y)$ denote the field of rational functions in x and y with rational coefficients and S the subfield consisting of the symmetric rational functions. $Q(N_a, N_b)$, $a \neq b$, is a subfield of S, and we will determine the dimension of the extension of S over $Q(N_a, N_b)$, denoted $[S : Q(N_a, N_b)]$. However, we have been unable to determine the dimension of S over $Q(N_a, N_b, N_c)$, though there is ample evidence for the following conjectures.

Conjecture 1. *Let a, b, c be distinct positive integers such that $(a, b, c) = 1$. Then $Q(N_a, N_b, N_c) = S$.*

We will settle this conjecture for a few infinite families of triplets a, b, c, but haven't settled even the following two special cases.

Conjecture 2. *Let b and c be integers, $1 < b < c$. Then $Q(N_1, N_b, N_c) = S$.*

Conjecture 3. *Let a, b, c be distinct positive integers such that $(a, b) = 1$. Then $Q(N_a, N_b, N_c) = S$.*

Throughout, the coefficients will be Q. If, for instance, the coefficient field has characteristic 2, the algebra will be quite different; then $N_1^2 = N_2$, but N_1 and N_2 are algebraically independent over Q.

1. The field generated by two Newton polynomials. Every symmetric polynomial in the ring $Q[x, y]$ is a polynomial in the elementary symmetric polynomials $S_1 = x + y$ and $S_2 = xy$. Since $S_1 = N_1$ and $S_2 = (N_1^2 - N_2)/2$, every symmetric polynomial is a polynomial in N_1 and N_2. Consequently, $Q(N_1, N_2) = S$. The iden-

Received by the editors on October 1, 1996.

tity $N_1^3 - N_3 = 3N_1S_2$ implies that $S_2 = (N_1^3 - N_3)/(3N_1)$. Thus $Q(N_1, N_3) = S$. These are the only cases when two Newton polynomials generate S, as Theorem 1.2 implies. For its proof we will need the following lemma.

Lemma 1.1. *Any two Newton polynomials N_a and N_b, $a < b$, are algebraically independent.*

Proof. Let u and v be indeterminates. By the degree of the monomial u^iv^j we shall mean $ai + bj$. Let $P(u, v)$ be a polynomial in $Q[u, v]$ of minimal degree such that $P(N_a, N_b) = 0$. We may assume that all the terms in $P(u, v)$ have the same degree. Furthermore, there is a term in $P(u, v)$ of the form cu^k, while all other terms have v as a factor.

Let ω be a primitive $2b$th root of 1. In the expression $P(N_a, N_b)$, replace y by $\omega^b x$, obtaining simply $c(1 + \omega^a)^k x^{ak}$, which is not 0. This contradiction establishes the lemma. □

Theorem 1.2. *Let $a < b$ be relatively prime positive integers. Then $[S : Q(N_a, N_b)] = ab/2$ if ab is even, and $a(b-1)/2$ if ab is odd.*

Proof. Let $u = x^a + y^a$ and $v = x^b + y^b$; hence, $y^a = u - x^a$ and $y^b = v - x^b$. Since $(a, b) = 1$, it follows that $y \in Q(u, v, x)$. All that remains, therefore, is to determine the degree of x over $Q(u, v)$, for that equals $[Q(x, y) : Q(N_a, N_b)]$, and $[S : Q(N_a, N_b)]$ is half of this dimension.

Since

$$(u - x^a)^b - (v - x^b)^a = 0,$$

x is algebraic over $Q(N_a, N_b)$ of degree at most ab. Note that the polynomial $(u - x^a)^b - (v - x^b)^a$, as a polynomial in the ring $Q(u, v)[x]$, has degree ab if ab is even and $a(b-1)$ if ab is odd.

We show that $p(u, v, x) = (u - x^a)^b - (v - x^b)^a$ is irreducible in $Q(u, v)[x]$.

Since $Z[u, v]$ is a unique factorization ring, it suffices to show that $p(u, v, x)$ is irreducible in $Z[u, v, x]$. So assume that $p(u, v, x) = q(u, v, x)r(u, v, x)$ where both $q(u, v, x)$ and $r(u, v, x)$ are in $Z[u, v, x]$.

For each integer i, we have

$$(u - i^a)^b - (v - i^b)^a = q(u,v,i)r(u,v,i).$$

By [**1**, p. 77], $(u - i^a)^b - (v - i^b)^a$ is irreducible in $Z[u,v,x]$. Thus, either $q(u,v,i)$ or $r(u,v,i)$ is 1 or -1. It follows that at least one of the polynomials $q(u,v,x)$ and $r(u,v,x)$ assumes the value 1 for an infinite number of choices of x or assumes the value -1 for an infinite number of choices of x. Consequently, one of those polynomials is identically 1 or identically -1 and hence $(u - x^a)^b - (v - x^b)^a$ is irreducible.

Thus $[Q(x,y) : Q(N_a, N_b)] = ab$ if ab is even and $a(b-1)$ if ab is odd. Since $[Q(x,y) : S] = 2$, the theorem follows. □

The next lemma reduces the computation of $[S : Q(N_a, N_b)]$ to the case when a and b are relatively prime.

Lemma 1.3. *Let a and b be distinct positive integers, with $(a,b) = d$. Then*

$$[S : Q(N_a, N_b)] = d^2[S : Q(N_{a/d}, N_{b/d})].$$

Proof. First consider $[Q(x,y) : Q(x^d, y^d)]$. Since x is a root of the equation $z^d - x^d = 0$ (where z is viewed as the variable), and y is a root of the equation $z^d - y^d = 0$, $[Q(x,y) : Q(x^d, y^d)] \le d^2$.

On the other hand, for each pair of dth roots of 1, ω and ω', the automorphism of $C(x,y)$ defined by $x \to \omega x$ and $y \to \omega' y$ leaves $C(x^d, y^d)$ elementwise fixed. Since $x + y$ has d^2 distinct images under these automorphisms, it does not satisfy an equation over $C(x^d, y^d)$ of degree less than d^2. Thus the degree of $x + y$ over $Q(x^d, y^d)$ is at least d^2. It follows that $[Q(x,y) : Q(x^d, y^d)] = d^2$.

Now

$$Q(N_a, N_b) \subseteq Q(x^d, y^d) \subseteq Q(x,y).$$

Since $[Q(x^d, y^d) : Q(N_a, N_b)] = [Q(x,y) : Q(N_{a/d}, N_{b/d})]$, the lemma follows. □

Corollary 1.4. *The only pairs of integers $a < b$ such that $Q(N_a, N_b) = S$ are $1, 2$ and $1, 3$.*

2. The implications for three Newton polynomials. The information concerning the field generated by two Newton polynomials, though inadequate to settle any of the three conjectures, does provide some evidence for their truth.

For instance, consider Conjecture 2. Assume that $(a, b) = 1$, $a < b$, and that ab is odd. Let k be a positive integer and $c = kab(b-1) - 1$. We will show that $Q(N_a, N_b, N_c) = S$.

Let $d = [Q(x, y) : Q(N_a, N_b, N_c)]$. We wish to show that $d = 2$. By Theorem 1.2,

$$d \mid a(b-1), \qquad d \mid b(c-1) \quad \text{and} \quad d \mid a(c-1).$$

Thus $d \mid c - 1$, that is, $d \mid kab(b-1) - 2$. It follows that $d \mid 2$, hence is 2.

If, instead, a is even and b is odd, let $c = kab - 1$. The same argument also justifies the case a odd and b even.

Similar reasoning provides an infinite number of cases for which Conjecture 3 holds. For instance, let b be even, c odd and $(b, c-1) = 2$. Then $Q(N_1, N_b, N_c) = S$. Similarly, if b and c are odd and $(b-1, c-1) = 2$, or if b and c are even and $(b, c) = 2$, the same conclusion holds.

The same technique applies to specific a and b. For instance, $Q(N_1, N_4, N_c) = S$ if $c \equiv 2$ or $3 \pmod 4$.

The same approach shows that if a is odd, then $Q(N_{a-1}, N_a, N_{a+1}) = S$. In a similar way, one may show that if a and b are even, c is odd, $(a, b) = 2$, $(a, c) = 1 = (b, c)$, then, again, $Q(N_a, N_b, N_c) = S$.

3. The ring generated by N_a, N_b, N_c. We now turn our attention to the ring $Q[N_a, N_b, N_c]$ generated by N_a, N_b, N_c. To each monomial $N_a^p N_b^q N_c^r$ we assign the degree $ap + bq + cr$. The vector space over Q spanned by the monomials of a given degree, d, form a vector space, $M(d)$, whose dimension we denote $m(d)$.

The vector space, $S(d)$, consisting of the symmetric polynomials of degree d has a basis consisting of $x^d + y^d, x^{d-1}y + xy^{d-1}, \dots$. Hence, its dimension is $(d+2)/2$ if d is even and $(d+1)/2$ if d is odd. These numbers are upper bounds for $m(d)$. If $2 \leq a < b < c$, $M(d)$ is not all of $S(d)$ since it does not contain $x^{d-1}y + xy^{d-1}$. As we will see, knowing the dimension $m(d)$ would probably settle Conjecture 1. The following lemma will be a tool in examining $m(d)$.

First note that there are nontrivial polynomials $P(u,v,w)$ such that $P(N_a, N_b, N_c) = 0$, since any three elements in $Q[x,y]$ are algebraically dependent [**1**, pp. 200–202]. (Or one could give a direct proof by showing that for large d the number of monomials of the form $N_a^p N_b^q N_c^r$ is (far) larger than the dimension of $S(d)$.)

Lemma 3.1. *Let a, b, c be distinct positive integers. Then $I = \{P(u,v,w) \in Q[u,v,w] : P(N_a, N_b, N_c) = 0\}$ is a principal ideal in $Q[u,v,w]$.*

Proof. Let p_u be a nonzero polynomial in I of smallest degree in u. We may assume that the only polynomials in $Q[v,w]$ that divide p_u are scalars, that is, elements of Q.

Now let $P \in I$. Then there are $q \in Q(v,w)[u]$ and $r \in Q(v,w)[u]$ such that $P = qp_u + r$ and either $r = 0$ or the degree of u in r is less than the degree of u in p_u. Write $q = q'(u,v,w)/d'(v,w)$ and $r = r^*(u,v,w)/d^*(v,w)$, where q', $r^* \in Q[u,v,w]$ and $d', d^* \in Q[v,w]$. We may assume that q' and d' are relatively prime and that r^* and d^* are relatively prime. Therefore,

$$P(u,v,w) = \frac{q'(u,v,w)p_u}{d'(v,w)} + \frac{r^*(u,v,w)}{d^*(v,w)}. \tag{1}$$

Since N_b and N_c are algebraically independent, we may replace u, v, w in Equation (1) by N_a, N_b, N_c and conclude that $r^* \in I$. By the minimality of p_u, $r^* = 0$. We conclude that

$$d'P = q'p_u.$$

But d' and q' are relatively prime and p_u has only scalar divisors in $Q[v,w]$. Thus $d' \in Q$, and it follows that P is a multiple of p_u in the ring $Q[u,v,w]$, and therefore I is a principal ideal in $Q[u,v,w]$. □

Note that p_u in the preceding proof is irreducible and homogeneous. In order not to favor any particular variable we denote it P' and denote its degree by d'.

Any nonzero polynomial $P(u,v,w)$ of degree d such that $P(N_a, N_b, N_c) = 0$ is a multiple of P' by a polynomial of degree $d - d'$.

For a positive integer d, let $W(d)$ be the vector space consisting of all polynomials in $Q[u,v,w]$ of degree d. Its dimension, which we denote $f(d)$, is the number of triplets x, y, z of nonnegative integers such that $ax + by + cz = d$.

Let $T : W(d) \to M(d)$ be defined by $T(u^p v^q w^r) = N_a^p N_b^q N_c^r$. Then for $d < d'$ the dimension of the kernel of T is 0 and for $d \geq d'$ is $f(d - d')$. In particular, for $d > d'$,

$$m(d) = f(d) - f(d - d'). \tag{2}$$

Euler investigated the function $f(d)$, using the identity

$$\frac{1}{1 - x^a} \frac{1}{1 - x^b} \frac{1}{1 - x^b} = \sum f(d) x^d.$$

With the aid of partial fractions over the complex field, and expanding each partial fraction as a power series, one can obtain a formula for $f(d)$. Letting $d_1 = (a,b)$, $d_2 = (a,c)$ and $d_3 = (b,c)$, we obtain the formula

$$f(d) = \frac{d^2}{2abc} + d(g_{d_1} + g_{d_2} + g_{d_3})(d) + (h_a + h_b + h_c)(d).$$

The g's and h's are functions with periods indicated by their subscripts; see, for instance, [**2**]. We conclude that

$$f(d) - f(d - d') = \frac{dd'}{abc} + h(d),$$

where h is a uniformly bounded function of d. Taking limits as $d \to \infty$ shows that $\lim_{d \to \infty} m(d)/d$ exists and that

$$\lim_{d \to \infty} \frac{m(d)}{d} = \frac{d'}{abc}.$$

Since $m(d)$ is not larger than $(d + 2)/2$, it follows that the degree of the minimal polynomial is at most $abc/2$.

On the basis of many examples computed by Dean Hickerson with the aid of Mathematica, we make the following conjecture.

Conjecture 4. *If $(a,b,c) = 1$, then the degree of the minimal polynomial for N_a, N_b and N_c is at least $2abc/5$.*

The truth of Conjecture 4 would imply the validity of Conjecture 1. To see this, note that there would then be three consecutive values of d for which $m(d) > (1/3)d$. Call these dimensions $n, n+1, n+2$. Pick a basis $b_1, b_2, \dots, b_r$ for $M(n)$ and a basis $c_1, c_2, \dots, c_s$ for $M(n+1)$. Then the $r+s$ polynomials $(x+y)b_1, (x+y)b_2, \dots, (x+y)b_r$, $c_1, c_2, \dots, c_s$ are linearly dependent, from which it follows that $x+y \in Q(N_a, N_b, N_c)$. A similar argument, using the dimensions n and $n+2$, shows that $xy \in Q(N_a, N_b, N_c)$, from which it follows that $S = Q(N_a, N_b, N_c)$. In all the computed cases there is such a dimension n less than $abc/2$.

REFERENCES

1. B.L. van der Waerden, *Modern algebra*, Volume 1, Frederick Ungar Publ. Co., New York, 1949.

2. Eugène Ehrhart, *Sur le nombre de solutions non négatives d'une equation diophantienne linéare*, Comptes Rendus Hebdomadaires des Séances de l'Acadamie des Sciences **256** (1963), 4566–4569.

Department of Mathematics, University of California at Davis, Davis, CA 95616-8633

Department of Mathematics, University of California at Davis, Davis, CA 95616-8633
E-mail address: stein@math.ucdavis.edu